UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,319	09/24/2003	Mark Delany	08226/100S142-US1	5654

7278   7590   12/16/2004

DARBY & DARBY P.C.
P. O. BOX 5257
NEW YORK, NY 10150-5257

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/671,319	DELANY, MARK
	Examiner	Art Unit	
	Ronald Baum	2136	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 6 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____ .

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-29* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-29* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-29 are pending for examination.

2.   Claims 1-29 are rejected.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. A "text record" is not a method. For the sake of applying art, the examiner assumes the rephrasing to capture the method aspect of the limitation. Correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5.   Claims 1-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Gupta et al, U.S. Patent 6,389,532 B1.

6.   As per claim 1; "A method for message authentication [Abstract, filtering so as to forward packets (i.e., messages) upon checking via public key encryption signature verification], comprising: generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain [Abstract, figures 4-8 and accompanying descriptions, whereas the key pair generated is clearly associated with the domain per se, and the DNS uses the public key to verify the signature.]; if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message [Abstract, figures 4-8 and accompanying descriptions, whereas the key pair generated is used to verify for the purpose of filtering messages (i.e., such that a message is forwarded or not as a function of the filtering results).]; and if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, providing the verified digitally signed message to the recipient [Abstract, figures 4-8 and accompanying descriptions, whereas again, the purpose of filtering messages is to enable forwarding or not as a function of the filtering results.].";

Further, as per claim 19; "A carrier wave signal that enables actions [This claim is the method embodied software (i.e., network download, etc., col. 2,lines 3-14) for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for message authentication, comprising: generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain; if a message originates from a sender's address associated with the domain,

employing a private component of the key pair to digitally sign the message and forwarding the

digitally signed message towards a recipient of the message; and if the public component stored

with the DNS verifies that the digitally signed message originated from the domain associated

with the sender's address, providing the verified digitally signed message to the recipient.".

Further, as per claim 29; "A method [This claim is the means plus function claim for the

method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for

enabling message authentication, comprising: means for enabling the generation of a key pair

associated with a domain, wherein a public component of the key pair is accessible to a domain

name server (DNS) that is associated with the domain; if a message originates from a sender's

address associated with the domain, means for enabling a private component of the key pair to be

employed to digitally sign the message and forwarding the digitally signed message towards a

recipient of the message; and if the public component stored with the DNS verifies that the

digitally signed message originated from the domain associated with the sender's address, means

for providing the verified digitally signed message to the recipient.".

7.   Claim 2 *additionally recites* the limitation that; "The method of Claim 1, further

comprising a text record that is accessible to the DNS and which includes at least the public

component of the key pair.". The teachings of Gupta et al are directed towards such limitations

(i.e., figures 4-8, and particularly figure 5, and accompanying descriptions, whereas the 'install

the public keys...' which clearly as stored in memory so as to be transferred from, as broadly

interpreted by the examiner would clearly encompass ' ... a text record ... DNS and which

includes ... public ... of the key pair ...'.).

8.   Claim 3 *additionally recites* the limitation that; "The method of Claim 1, further

comprising generating a selector that is associated with the key pair, wherein the selector is

employable to identify the key pair's public component for accessing by the DNS.". The

teachings of Gupta et al are directed towards such limitations (i.e., figures 4-8, and particularly

figure 5, and accompanying descriptions, whereas the 'distribute ... keys...' which clearly

indicate that the key pairs can be selected as a function of (i.e., in a multicast, at the very least,

environment) specifically designated nodes, as broadly interpreted by the examiner would clearly

encompass ' ... selector ... associated with the key pair, ... identify the key ... public component

... DNS ...'.).

          Further, as per claim 20 *additionally reciting* the limitation that; "The carrier wave signal

[This claim is the method embodied software (i.e., network download, etc., col. 2,lines 3-14) for

the method claim 3 above, and is rejected for the same reasons provided for the claim 3

rejection] The carrier wave signal of Claim 19, further comprising generating a selector that is

associated with the key pair, wherein the selector is employable to identify the key pair's public

component for accessing by the DNS.".

9.   Claim 4 *additionally recites* the limitation that; "The method of Claim 3, further

comprising forming a lookup query for the DNS by combining the selector with the sender's

address.". The teachings of Gupta et al are directed towards such limitations (i.e., figures 4-8,

and particularly figure 5, and accompanying descriptions, whereas the 'create ... keys ... store in

indexed tables ...' which clearly indicate that the key pairs can be selected from an indexed table

(i.e., database, flat or otherwise) as a function of specifically designated nodes (i.e., the associated IP addresses), as broadly interpreted by the examiner would clearly encompass ' ... lookup query ... DNS by combining the selector ... sender's address ...'.).

10.   Claim 5 *additionally recites* the limitation that; "The method of Claim 1, further comprising employing a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.". The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and accompanying descriptions, whereas the '... filter point, such as a router or firewall to an *intranet* ...' which clearly indicate that the messages pass through controlled intermediaries, as broadly interpreted by the examiner would clearly encompass ' ... mail server ... forward the ... message towards the recipient of the message ...'.).

11.   Claim 6 *additionally recites* the limitation that; "The method of Claim 1, further comprising employing a mail server associated with the domain to employ the private component of the key pair to digitally sign the message.". The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and accompanying descriptions, whereas the '... filter point, such as a router or firewall to an *intranet* ...' which clearly indicate that the messages pass through *controlling intermediaries*, such that the filtering done via digitally signed message verification is done by said *controlling intermediaries*, as broadly interpreted by the examiner would clearly encompass ' ... mail server ... employ the private ... key pair to digitally sign the message ...'.).

12.   Claim 7 *additionally recites* the limitation that; "The method of Claim 1, further comprising employing a mail server that is associated with a domain of the recipient to verify the domain of origination for the message with the public component of the key pair.". The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and accompanying descriptions, whereas the '... filter point, such as a router or firewall to an *intranet* ...' which clearly indicate that the messages pass through *controlling intermediaries*, such that the filtering done via digitally signed message verification is done by said *controlling intermediaries* (more particularly in this case 'closer' to the destination then the source), as broadly interpreted by the examiner would clearly encompass ' ... mail server ... recipient to verify ... origination ... public component ... key pair ...'.).

13.   Claim 8 *additionally recites* the limitation that; "The method of Claim 1, further comprising employing a mail server that is associated with a domain of the recipient to provide the verified digitally signed message to the recipient.". The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and accompanying descriptions, whereas the '... filter point, such as a router or firewall to an *intranet* ...' which clearly indicate that the messages pass through *controlling intermediaries*, such that the filtering and *subsequent forwarding of the message thereof*, done via digitally signed message verification is done by said *controlling intermediaries* (more particularly in this case 'closer' to the destination then the source), as broadly interpreted by the examiner would clearly encompass ' ... mail server ... recipient to provide the ... message to the recipient ...'.).

14.   Claim 9 *additionally recites* the limitation that; "The method of Claim 1, further

comprising accessing the public component of the key pair by employing a text record in a look

up table for the DNS.". The teachings of Gupta et al are directed towards such limitations (i.e.,

figures 4-8, and particularly figure 5, and accompanying descriptions, whereas the 'install the

public keys...' which clearly as stored in memory so as to be transferred from, as broadly

interpreted by the examiner would clearly encompass ' ... accessing ... public ... key ... text

record in a look up table for the DNS. ...'.).

15.   Claim 10 *additionally recites* the limitation that; "The method of Claim 1, further

comprising generating a plurality of key pairs associated with the domain, wherein at least two

key pairs are associated with at least two different senders and wherein each public component

of each key pair is accessible by the DNS associated with the domain.". The teachings of Gupta

et al are directed towards such limitations (i.e., Abstract, figures 1-8, and accompanying

descriptions, whereas the '... filter point, such as a router or firewall to an *intranet* ...' whereby

the messages pass through controlled intermediaries, insofar as the network consists of a

plurality of sender/recipient nodes of which common DNS/intermediaries (utilized in the

filtering), clearly teaches the use of the claim limitation plural node aspects (i.e.,

sender/intermediary/recipient in a multicast environment) as broadly interpreted by the examiner,

and would clearly encompass ' ... plurality of key pairs ... at least two different senders ... key

... accessible by the DNS associated with the domain ...'.);

Further, as per claim 21 *additionally reciting* the limitation that; "The carrier wave Signal

[This claim is the method embodied software (i.e., network download, etc., col. 2,lines 3-14) for

the method claim 10 above, and is rejected for the same reasons provided for the claim 10

rejection] of Claim 19, further comprising generating a plurality of key pairs associated with the

domain, wherein at least two key pairs are associated with at least two different senders and

wherein each public component of each key pair is accessible by the DNS associated with the

domain.".

16.   Claim 11 *additionally recites* the limitation that; "The method of Claim 10, further

comprising separately associating private components of the at least two key pairs with at least

two mail servers, wherein the at least two mail servers are associated with the domain.". The

teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and

accompanying descriptions, whereas the '... filter point, such as a router or firewall to an

intranet ...' whereby the messages pass through controlled intermediaries, insofar as the network

consists of a *plurality* of sender/recipient nodes of which common DNS/intermediaries (utilized

in the filtering, at the individual *router or firewall* nodes), clearly teaches the use of the claim

limitation plural node aspects (i.e., sender/intermediary/recipient in a multicast environment) as

broadly interpreted by the examiner, and would clearly encompass ' ... separately ... private ...

at least two key pairs with at least two mail servers, ... domain ...'.);

Further, as per claim 22 *additionally reciting* the limitation that; "The carrier wave signal·

[This claim is the method embodied software (i.e., network download, etc., col. 2,lines 3-14) for

the method claim 11 above, and is rejected for the same reasons provided for the claim 11

·rejection] of Claim 21, further comprising separately associating private components of the at least two key pairs with at least two mail servers, wherein the at least two mail servers are associated with the domain.".

17.   Claim 12 *additionally recites* the limitation that; "The method of Claim 10, wherein each private component of each key pair employs a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.". The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and accompanying descriptions, whereas the '... filter point, such as a router or firewall to an *intranet* ...' whereby the messages pass through controlled intermediaries, insofar as the network consists of a *plurality* of sender/recipient nodes of which common DNS/intermediaries (utilized in the *filtering and forwarding*, irrespective of the source or destination node proximity to any given individual *router or firewall* nodes), clearly teaches the use of the claim limitation plural node aspects (i.e., sender/intermediary/recipient in a multicast environment) as broadly interpreted by the examiner, and would clearly encompass ' ... private ... key ... mail server associated ... to forward the ... message towards the recipient of the message ...'.);

      Further, as per claim 23 *additionally reciting* the limitation that; "The carrier wave signal [This claim is the method embodied software (i.e., network download, etc., col. 2, lines 3-14) for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection] of Claim 21, wherein each private component of each key pair employs a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.".

18. Claim 13 *additionally recites* the limitation that; "The method of Claim 1, further comprising employing one of a plurality of mail servers associated with the domain to digitally sign the message with the private component of the key pair and forward the digitally signed message towards the recipient.". The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and accompanying descriptions, whereas the '... filter point, such as a router or firewall to an *intranet* ...' whereby the messages pass through controlled intermediaries, insofar as the network consists of a *plurality* of sender/recipient nodes of which common DNS/intermediaries (utilized in the *filtering and forwarding*, irrespective of the source or destination node proximity to any given individual *router or firewall* nodes), clearly teaches the use of the claim limitation plural node aspects (i.e., sender/intermediary/recipient in a multicast environment) as broadly interpreted by the examiner, and would clearly encompass ' ... plurality of mail servers ... sign the message ... private ... key ... forward ... message towards the recipient ...'.).

19. As per claim 14; "A system for message authentication, comprising [This claim is the combination of claims 1,5-8 above, and is rejected for the same reasons provided for the claims 1,5-8 rejection]: a client that is enabled to generate at least one message for a recipient, wherein the client is associated with a domain; a mail server associated with the domain of the client, wherein the mail server performs actions, including: enabling the generation of a key pair associated with the domain, wherein a public component of the key pair is accessible to a DNS that is associated with the domain; and if a message from the client originates from the domain,

enabling a private component of the key pair to digitally sign the message and forward the

digitally signed message towards the recipient of the message; and a mail server associated with

a domain of the recipient, wherein the mail server performs actions including enabling the public

component stored with the DNS to verify that the digitally signed message originated from the

domain associated with the client, and enabling each verified digitally signed message to be

provided to the recipient.".

20.   Claim 15 *additionally recites* the limitation that; "The system of claim 14, wherein the

message is at least one of an email, instant message (IM), short message service (SMS).". (i.e.,

Abstract, figures 1-8, and accompanying descriptions, whereas the packet messages per se, in the

aggregate, form larger messages, as broadly interpreted by the examiner, and would clearly

encompass ' ... email ...'.).

21.   Claim 16 *additionally recites* the limitation that; "The system of Claim 14, further

comprises a text record that is accessible to the DNS and which includes at least the public

component of the key pair.". The teachings of Gupta et al are directed towards such limitations

(i.e., figures 4-8, and particularly figure 5, and accompanying descriptions, whereas the 'install

the public keys...' which clearly as stored in memory so as to be transferred from, as broadly

interpreted by the examiner would clearly encompass ' ... a text record ... DNS and which

includes ... public ... of the key pair ...'.).

22.   Claim 17 *additionally recites* the limitation that; "The system of Claim 14, further

comprises a selector that is associated with the key pair, wherein the selector is employable to

identify the key pair's public component for accessing by the DNS.". The teachings of Gupta et

al are directed towards such limitations (i.e., figures 4-8, and particularly figure 5, and

accompanying descriptions, whereas the 'distribute ... keys...' which clearly indicate that the

key pairs can be selected as a function of (i.e., in a multicast, at the very least, environment)

specifically designated nodes, as broadly interpreted by the examiner would clearly encompass '

... selector ... associated with the key pair, ... identify the key ... public component ... DNS

...'.).

23.   Claim 18 *additionally recites* the limitation that; "The system of Claim 14, further

comprising a plurality of key pairs that are associated with at least two different clients, wherein

each public component of each key pair is accessible by the DNS associated with the domain.".

The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and

accompanying descriptions, whereas the '... filter point, such as a router or firewall to an

intranet ...' whereby the messages pass through controlled intermediaries, insofar as the network

consists of a *plurality* of sender/recipient nodes of which common DNS/intermediaries (utilized

in the filtering), clearly teaches the use of the claim limitation plural node aspects (i.e.,

sender/intermediary/recipient in a multicast environment) as broadly interpreted by the examiner,

and would clearly encompass ' ... plurality of key pairs ... at least two different senders ... key

... accessible by the DNS associated with the domain ...'.).

24.   As per claim 24; "A client that enables message authentication, comprising [This claim is

the claim 1 above such that the client perspective is recited as the distinguishing limitation

difference, and is rejected for the same reasons provided for the claim 1 rejection, insofar as the

teachings of Gupta et al are clearly directed towards the client and server implementations of the

network sending/receiving nodes.]: enabling the generation of a key pair associated with a

domain, wherein a public component of the key pair is accessible to a domain name server

(DNS) that is associated with the domain; if a message originates from a sender's address

associated with the domain, enabling a private component of the key pair to be employed to

digitally sign the message and forwarding the digitally signed message towards a recipient of the

message; and if the public component stored with the DNS verifies that the digitally signed

message originated from the domain associated with the sender's address, providing the verified

digitally signed message to the recipient.".

25.   Claim 25 *additionally recites* the limitation that; "The client of Claim 24, further

comprising enabling the generation of a plurality of key pairs associated with the domain,

wherein at least two key pairs are associated with at least two different senders and wherein each

public component of each key pair is accessible by the DNS associated with the domain.". The

teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and

accompanying descriptions, whereas the '... filter point, such as a router or firewall to an

intranet ...' whereby the messages pass through controlled intermediaries, insofar as the network

consists of a *plurality* of sender/recipient nodes of which common DNS/intermediaries (utilized

in the filtering), clearly teaches the use of the claim limitation plural node aspects (i.e.,

sender/intermediary/recipient in a multicast environment) as broadly interpreted by the examiner,

and would clearly encompass ' ... plurality of key pairs ... at least two different senders ... key

... accessible by the DNS associated with the domain ...'.).

26.   Claim 26 *additionally recites* the limitation that; "The client of Claim 25, further

comprising enabling the separate association of private components of the at least two key pairs

with at least two mail servers, wherein the at least two mail servers are associated with the

domain.". The teachings of Gupta et al are directed towards such limitations (i.e., Abstract,

figures 1-8, and accompanying descriptions, whereas the '... filter point, such as a router or

firewall to an *intranet* ...' whereby the messages pass through controlled intermediaries, insofar

as the network consists of a *plurality* of sender/recipient nodes of which common

DNS/intermediaries (utilized in the filtering, at the individual *router or firewall* nodes), clearly

teaches the use of the claim limitation plural node aspects (i.e., sender/intermediary/recipient in a

multicast environment) as broadly interpreted by the examiner, and would clearly encompass '

... separately ... private ... at least two key pairs with at least two mail servers, ... domain ...'.).

27.   Claim 27 *additionally recites* the limitation that; "The client of Claim 25, further

comprising enabling each private component of each key pair to employ a mail server associated

with the domain to forward the digitally signed message towards the recipient of the message.".

The teachings of Gupta et al are directed towards such limitations (i.e., Abstract, figures 1-8, and

accompanying descriptions, whereas the '... filter point, such as a router or firewall to an

intranet ...' whereby the messages pass through controlled intermediaries, insofar as the network

consists of a *plurality* of sender/recipient nodes of which common DNS/intermediaries (utilized in the *filtering and forwarding*, irrespective of the source or destination node proximity to any given individual *router or firewall* nodes), clearly teaches the use of the claim limitation plural node aspects (i.e., sender/intermediary/recipient in a multicast environment) as broadly interpreted by the examiner, and would clearly encompass ' ... private ... key ... mail server associated ... to forward the ... message towards the recipient of the message ...'.).

28.   As per claim 28; "A server that enables message authentication, comprising [This claim is the claim 1 above such that the client perspective is recited as the distinguishing limitation difference, and is rejected for the same reasons provided for the claim 1 rejection, insofar as the teachings of Gupta et al are clearly directed towards the client and server implementations of the network sending/receiving nodes.]: enabling the generation of a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain; if a message originates from a sender's address associated with the domain, enabling a private component of the key pair to be employed to digitally sign the message and forwarding; the digitally signed message towards a recipient of the message; and if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, providing the verified digitally signed message to the recipient.".

Conclusion

29.   Any inquiry concerning this communication or earlier communications from examiner

should be directed to Ronald Baum, whose telephone number is (571) 272-3681, and whose

unofficial Fax number is (571) 273-3681. The examiner can normally be reached Monday

through Friday from 8:00 AM to 5:30 PM.

     If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization

where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner